

УДК 621.371

СОЗДАНИЕ ТЕСТОВЫХ РЕЖИМОВ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПЭВМ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

А.Г. ФИЛИППОВИЧ, К.К. ШУЛЬГАН

*Оперативно-аналитический центр при Президенте Республики Беларусь,
Кальварийская, 17, Минск, 220004, Беларусь*

Поступила в редакцию 20 апреля 2011

Рассматриваются методы создания тестовых режимов интерфейсов ПЭВМ в целях оценки защищенности информации от утечки по каналам побочных электромагнитных излучений. Предложенный подход к созданию тестовых режимов позволяет создавать максимально возможный уровень побочных электромагнитных излучений, источниками которых являются интерфейсы ПЭВМ, передающие информацию с помощью последовательностей импульсов. Возможность создания и применения таких режимов для оценки защищенности ПЭВМ теоретически и экспериментально исследована для видеointерфейса SVGA.

Ключевые слова: побочные электромагнитные излучения, интерфейс, тестовый режим.

Введение

В настоящее время основным средством обработки информации во всех сферах деятельности общества является ПЭВМ. Часто обрабатываемая информация в средствах вычислительной техники носит конфиденциальный характер. В этом случае к средствам обработки информации необходимо предъявлять требования по защищенности от различного рода угроз информационной безопасности.

Одним из основных каналов утечки информации в средствах вычислительной техники являются каналы побочных электромагнитных излучений [1]. Их образование связано с тем, что в средствах вычислительной техники информация обрабатывается и передается с помощью электрических сигналов, циркулирующих в аппаратных устройствах и интерфейсах средств вычислительной техники. Указанные электрические сигналы являются источниками электромагнитных полей, излучаемыми ПЭВМ. Как показывают исследования [1-5], информация, передаваемая побочными электромагнитными излучениями, может быть перехвачена средствами разведки на расстояниях десятков и сотен метров, и зачастую этого расстояния достаточно для установки средств разведки. В этой связи видится необходимым осуществлять оценку опасности побочных электромагнитных излучений ПЭВМ до начала обработки информации с целью определения необходимых мероприятий для защиты информации.

Оценка защищенности информации от утечки по каналу побочных электромагнитных излучений

Как правило, защищенность информации, обрабатываемой ПЭВМ, от утечки по каналам побочных электромагнитных излучений определяется таким параметром, как отношение сигнала к шуму на входе приемного устройства средства разведки [1, 6]:

$$q = \frac{U_c \sqrt{\Delta F}}{U_{ш}(\Delta F)}, \quad (1)$$

где U_c – напряжение сигнала на входе разведывательного приемника, $U_{ш}(\Delta F)$ – напряжение шумов на входе разведывательного приемника, измеренное в полосе частот ΔF , ΔF – ширина спектра тестового сигнала, F_T – тактовая частота тестового сигнала. Напряжение тестового сигнала на входе разведывательного приемника для электрической и магнитной составляющих электромагнитного поля рассчитывается по формулам [6]:

$$U_{ci} \approx \frac{h_a}{2} \sqrt{\sum_{\Delta F_i} \left(\frac{E_{cj}}{V_j(R)} \right)^2}, \quad U_{ci} \approx \frac{h_a}{2} \sqrt{\sum_{\Delta F_i} \left(\frac{\rho H_{cj}}{V_j(R)} \right)^2}, \quad (2)$$

где E_{cj} , H_{cj} – напряженности электрической и магнитной составляющих электромагнитного поля тестового сигнала на j -й частоте в частотном интервале ΔF_i в точке проведения измерений соответственно, h_a – действующая высота антенны разведывательного приемника, $V_j(R)$ – коэффициент затухания электромагнитного поля, R – расстояние от средства вычислительной техники.

Для определения отношения сигнала к шуму с помощью выражений (1) и (2) необходимо провести измерения векторов напряженностей побочных электромагнитных излучений ПЭВМ. Однако, как показывают исследования [6], интенсивность побочных электромагнитных излучений при штатных режимах обработки информации в ПЭВМ относительно невелика, и средствами радиоизмерений широкого назначения трудно провести необходимые измерения. В этой связи существует потребность в том, чтобы создать такие режимы обработки информации в ПЭВМ, при которых уровень побочных электромагнитных излучений был бы максимален.

Принципы формирования тестовых режимов

Необходимо отметить, что основные интерфейсы, опасные с точки зрения перехвата информации по каналам побочных электромагнитных излучений, используют для обработки и передачи информации импульсные сигналы [6]. Наиболее мощным источником побочных электромагнитных излучений, пригодных для перехвата и восстановления обрабатываемой информации, является видеотракт ПЭВМ [6], поэтому рассмотрим принципы формирования тестовых режимов передачи информации на примере этого интерфейса. Для других интерфейсов принципы формирования тестовых сигналов будут аналогичными.

Определим условия, при которых ПЭВМ будет излучать побочные электромагнитные излучения, источником которых является видеоинтерфейс ПЭВМ, с максимальной интенсивностью, исходя из рассмотрения структуры сигнала видеоизображения. Схематически временная структура аналогового видеосигнала, передаваемого по интерфейсу SVGA, изображена на рис. 1. Каждая строка видеоизображения кодируется в виде трех амплитудно-модулированных последовательностей видеоимпульсов, передающих информацию о яркости каждого из трех цветов отображаемого пикселя. Строки изображения в структуре видеосигнала отделены интервалами гашения, строчной и кадровой синхронизации. Физически информация, отображаемая на экране монитора ПЭВМ, передается от видеоадаптера, расположенного в системном блоке, к монитору по трем коаксиальным линиям. Из-за рассогласования в местах стыков разъемов кабеля интерфейса и корпусов системного блока и монитора ПЭВМ на экранированной поверхности кабеля интерфейса возникает электрический ток, являющийся источником побочных электромагнитных излучений.

Видеоимпульсы передаются с частотой следования пикселей f_p , определяемой по формуле [3]:

$$f_p = f_v x_t y_t, \quad (3)$$

где f_v – частота следования кадров, x_t и y_t – горизонтальный и вертикальный размеры экрана в пикселях с учетом интервалов следования синхроимпульсов и интервалов гашения. Частота следования пикселей также приближенно может быть выражена в виде [5]:

$$f_p \approx 1,35 f_v x_d y_d, \quad (4)$$

где x_d и y_d – горизонтальное и вертикальное разрешение экрана в пикселях.

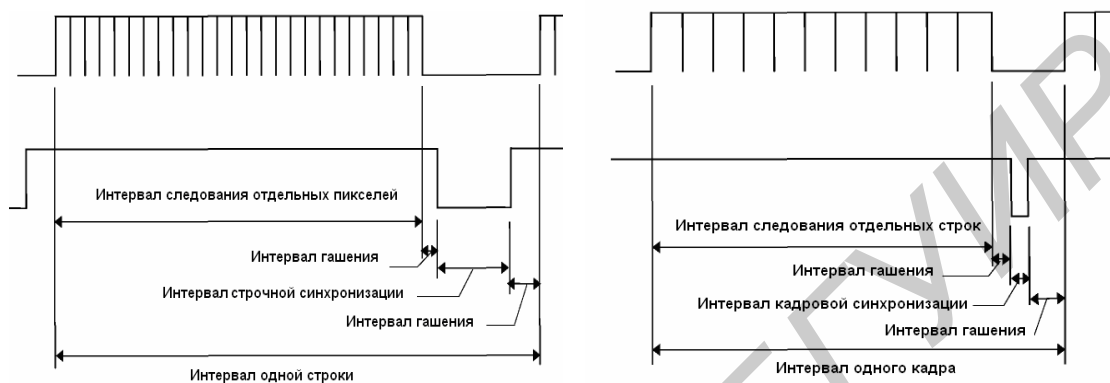


Рис. 1. Временная структура аналогового видеосигнала

Спектр последовательности прямоугольных видеоимпульсов, передаваемых по интерфейсу SVGA, может быть представлен следующим выражением [7]:

$$S(f) = |S_0(f)| |S_\xi(f)| = t_u \left| \frac{\sin(\pi f t_u)}{\pi f t_u} \right| \left| \frac{\sin(\pi n f T_n)}{\sin(\pi f T_n)} \right|, \quad (5)$$

где $S_0(f)$ – спектр одиночного видеоимпульса, $S_\xi(f)$ – спектр огибающей последовательности прямоугольных видеоимпульсов, f – частота, $T_n \approx \frac{k}{f_p}$ – период следования импульсов, k – скважность импульсов, принимающая значения только из множества натуральных чисел, $t_u \approx \frac{1}{f_p}$ – длительность импульса, n – число импульсов в последовательности.

Очевидно, что для получения гармоник в спектре видеосигнала с максимально возможной амплитудой необходимо, чтобы максимумы функций $S_0(f)$ и $S_\xi(f)$ совпадали. Определим условия совпадения максимумов функций $S_0(f)$ и $S_\xi(f)$. Рассмотрим функцию $S_0(f)$. Производная этой функции определяется следующим выражением:

$$S'_0(f) = \frac{f \cos(\pi f t_u) - \sin(\pi f t_u)}{\pi f^2}. \quad (6)$$

Графики функций $S_0(f)$ и $S'_0(f)$ показаны на рис. 2. Очевидно, что максимумы функции $S_0(f)$ будут на частотах, при которых функция $S'_0(f)$ имеет нулевые значения. Анализ выражения (6) показывает, что приближенно эти частоты могут быть определены из следующего выражения:

$$f_{S'_0=0} \approx \frac{m f_p}{2}, \quad (7)$$

где m – множество натуральных нечетных чисел.

Рассмотрим функцию $S_{\xi}(f)$. Выясним, на каких частотах функция $S_{\xi}(f)$ принимает максимальные значения.

Очевидно, что максимумы функция $S_{\xi}(f)$ будет иметь в случаях, когда знаменатель функции равен нулю, то есть на частотах

$$f = \frac{l}{T_n} = \frac{l}{k} f_p, \quad (8)$$

где l – множество действительных чисел.

Функция $S_{\xi}(f)$ на этих частотах представляет собой неопределенность типа $\frac{0}{0}$.

Разрешим эту неопределенность, применяя к пределу функции $S_{\xi}(f)$ при $f \rightarrow \frac{l}{T_n}$ правило Лопиталя:

$$\lim(S_{\xi}(f))_{f \rightarrow \frac{l}{T_n}} = \lim \frac{\sin'(\pi n f T_n)}{\sin'(\pi f T_n)}_{f \rightarrow \frac{l}{T_n}} = n \frac{\cos(\pi n l)}{\cos(\pi l)} = n. \quad (9)$$

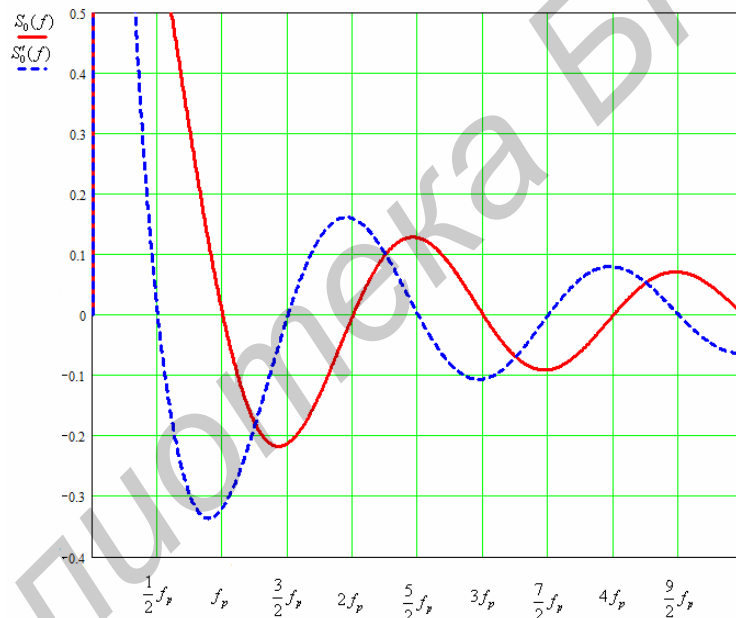


Рис. 2. Графики функций $S_0(f)$ и $S'_0(f)$

Определим, при каких условиях максимумы функций $S_{\xi}(f)$ и $S_0(f)$ совпадут. Для этого приравняем выражения (7) и(8). Получим:

$$\frac{m}{2} f_p = \frac{l}{k} f_p. \quad (10)$$

Поскольку m – множество натуральных нечетных чисел, для обеспечения равенства (10) необходимо, чтобы величина k была кратной двум. Следовательно, для обеспечения условия совпадения максимумов функций $S_{\xi}(f)$ и $S_0(f)$ необходимо формировать тестовые последовательности видеоимпульсов со скважностью, кратной двум. При этом использование последовательности импульсов со скважностью, равной двум, имеет ряд преимуществ. Во-первых, при одинаковых длительностях сигналов амплитуда спектральных гармоник на частотах максимума кратна числу импульсов сигнала. Следовательно, чем меньше скважность, тем больше количество импульсов в сигнале, и больше амплитуда спектральных гармоник. Кроме

того, с увеличением значения скважности импульсов, в соответствии с (8), увеличивается количество максимумов функций $S_{\xi}(f)$. Следовательно, энергия сигнала будет распределяться на дополнительные гармоники, которые расположены на частотах, отличных от частот максимумов функции $S_0(f)$.

Результаты математического моделирования и эксперимента для интерфейса SVGA

На рис. 3 показаны теоретический и экспериментальный спектры тестовой последовательности видеоимпульсов со скважностью, равной двум, при разрешении видеоизображения 800x600x75 Гц.

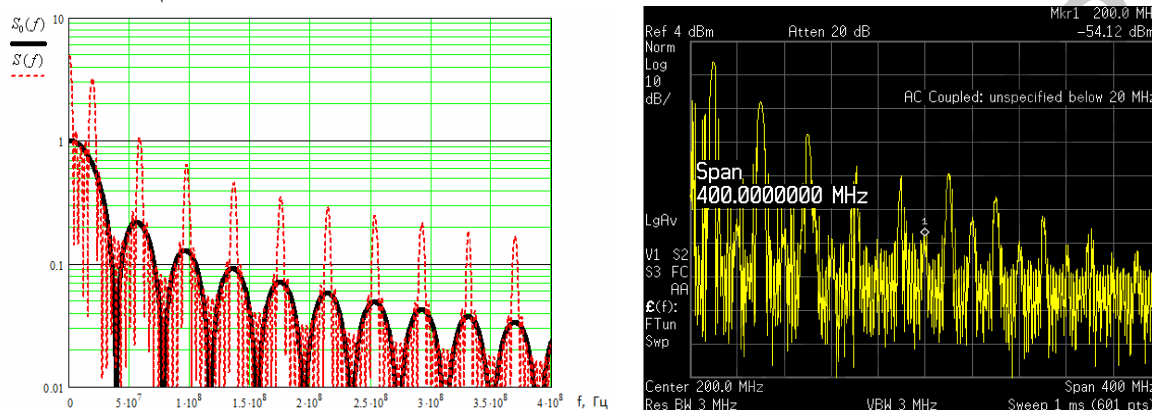


Рис. 3. Расчетный и экспериментальный спектры тестовых сигналов интерфейса SVGA

Тестовый сигнал в спектральной области представляет собой совокупность гармоник, отстоящих друг от друга по частоте на f_p , убывающих с ростом частоты. Для изменения положения гармоник тестового сигнала на оси частот необходимо изменять значение f_p . Варьировать значения f_p , в соответствии с (4), можно изменением параметров разрешения видеоизображения.

На рис. 4 показан типичный спектр сигнала побочных электромагнитных излучений, полученный с помощью анализатора спектра и измерительной антенны на частоте $\frac{5}{2}f_p$.

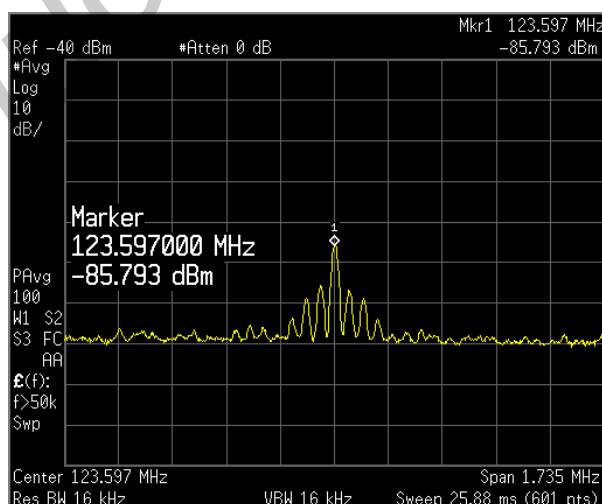


Рис. 4. Спектр сигнала побочных электромагнитных излучений на частоте $\frac{5}{2}f_p$, полученный с помощью анализатора спектра и измерительной антенны

Эксперимент показал, что в большинстве случаев использование тестовых сигналов позволяет создать необходимый уровень напряженностей электромагнитного поля для проведе-

ния измерений в диапазоне частот 40–800 МГц. При этом обеспечивается хорошее распознавание опасного сигнала как по форме спектра, так и по факту появления и исчезновения излучения при включении и выключении тестового сигнала. Максимальные значения вектора напряженности электрического поля побочных электромагнитных излучений экспериментально были зафиксированы на частотах 80–300 МГц, которые можно признать наиболее опасными с точки зрения возможного перехвата информации средствами разведки. Опасность перехвата информации в этом диапазоне частот объясняется следующими факторами. Во-первых, амплитуды гармоник сигнала видеоизображения в этом диапазоне частот имеют относительно высокую амплитуду. Во-вторых, в указанном диапазоне частот находятся резонансные частоты соединительных кабелей видеоинтерфейсов ПЭВМ.

Предложенные в настоящей статье подходы могут быть использованы для формирования тестовых последовательностей, необходимых для оценки защищенности информации от утечки по каналам побочных электромагнитных излучений, любых интерфейсов средств вычислительной техники, информация по которым передается в виде последовательностей импульсов.

CREATION OF TEST REGIMES TO ESTIMATE THE SECURITY OF PERSONAL COMPUTERS FROM LEAKING THROUGH THE SIDE ELECTROMAGNETIC RADIATION

A.G. FILIPPOVICH, K.K. SHULGAN

Abstract

Creation of the test interface mode in order to estimate security of information leakage of PC through the side electromagnetic radiation was considered. The proposed approach to the creation of test mode allows to create the highest possible level of electromagnetic radiation originating from the PC interface transmit information using a series of pulses. Ability to create and use these regimes to assess the security of personal computers theoretically and experimentally investigated for the SVGA interface.

Литература

1. *Пятчиков А.Г.* Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам. М., 2007
2. *W. van Eck* // *Computers&Security*. 1985. №4. P. 269–286.
3. *Kuhn M.G.* Technical report UCAM-CL-TR-577, 2003.
4. *Tanaka H., Takizawa O., Yamamura A.* // *Journal of the Institute of Image Electronics Engineers of Japan*. 2005. Vol. 34, №2. P. 213–223.
5. *Tanaka H., Takizawa O., Yamamura A.* // *Information security applications*. 2005. Vol. 3325. P. 457–469.
6. *Хорев А.А.* // *Специальная техника*. 2007. №4, P. 56–64.
7. *Атабеков Г.И.* Основы теории цепей. М., 1969.